UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,096	12/05/2003	Anders M. E. Samuelsson	MS1-1696US	8822

22801 7590 02/04/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
YOUNG, NICOLE M	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
02/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,096	SAMUELSSON ET AL.	
	Examiner	Art Unit	
	Nicole M. Young	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5, 8-17, and 19 -32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 8-17, and 19 -32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/23/2007 and 10/16/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

In view of the appeal brief filed on October 16, 2007, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

This communication is in response to the amendment filed on 2/23/2007. Claims 1-5, 8-17, and 19-32 are pending. Claims 6-7 and 18 are cancelled. Claims 1-3, 5, 14-17, 22 and 28-32 are amended.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 22 teaches a system comprised of a first security engine, a second security engine and an event manager. The specification defines security engines as "implemented in software, hardware, or a combination of both." It is further stated, that the event manager receives events from the security engines and then "processes these events and communicates the information contained in particular events to other search engines." The Examiner interprets the event manager to recite software. Therefore, the entire claim recites software, which fails to fall into one of the 4 categories of invention. The dependent claims 23-27 limit the software of independent claim 22, so they are non-statutory as well.

The rejection for claims 22-27 under 35 U.S.C. 101 stands as the amendment filed 2/23/2007 does not recite enough structure. The Examiner suggests modeling claim 22 after statuary claim 28.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 14-17, 19-21, and 28-32 are rejected under 35 U.S.C. 102(e) as being anticipated by **Willebeek-LeMair et al. (US 2003/0204632 A1)** hereinafter Willebeek-LeMair.

Claim 14:

Paragraph [0014] teaches an intrusion detector functionality that sends an alert when detecting potentially harmful traffic. This is sent to a firewall, which responds by blocking the entrance of the detected traffic. The Examiner interprets the intrusion detector and firewall to be "security engines" of claim 1. This would then teach one security engine (intrusion detector) detecting an event (potentially harmful traffic), identifying a second security engine (firewall), and communicating the event to it. Paragraph [0075] teaches that the network discovery functionality maintains a database

that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information.

Claim 15:

Figure 6 and associated text especially paragraph [0081] disclose information of whether a connection is wired or wireless.

Claim 16:

Figure 6 and associated text especially paragraph [0081] disclose information of whether a connection corporate (intranet).

Claim 17:

Figure 6 and associated text especially paragraph [0081] disclose information of whether a connection unknown.

Claim 19:

Paragraph [0075] teaches that the network discovery functionality maintains a database that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information. The paragraph later states "this information is then used by the system 110, in view of the detection signatures 132, to adapt the operation of the intrusion detector functionality 116 and firewalling functionality 118 by tailoring the signatures in the context of the network configuration." The Examiner interprets this as the two security engines using system state information stored in a shared database.

Claim 20:

Paragraph [0012] teaches a firewall, IDS, and VAS system integrated into one system. The Examiner interprets this as three security engines communicating. Paragraph [0013] further states "the present invention integrates a network discovery functionality, an intrusion detector functionality and a firewalling functionality together such that a self-deploying and self-hardening security defense is provided for a network. Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations." This further teaches three integrated security engines.

Claim 21:

Paragraph [0012] teaches a "single vendor solution" integrating the security components. This could be interpreted by one of ordinary skill in the art at the time of invention to be a computer program.

Claim 28:

Figure 2 shows a network defense system that includes a security management agent and two security engines (an intrusion detector functionality and a firewalling functionality). As shown the security management agent has the functionality to receive alerts from one of the security engines listed and communicate the alert to the other. Paragraph 81 explains the implementation of system 10 in Figure 2. It teaches a threat prevention appliance 500 that utilizes system 10 and is "configured as a network element in the protected network 14." The Examiner interprets this functionality as a computer program and the network element as a computer-readable medium. Paragraph [0075] teaches that the network discovery functionality maintains a database

that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information.

Claim 29:

Paragraph [0014] states "content that is potentially harmful to the network." The Examiner interprets this to be "a type of security attack" as in claim 29.

Claim 30:

Paragraph [0075] teaches an "enterprise vulnerabilities databases that stores the enterprise specific data collected by the network discovery functionality." It later states that the stored data may comprise "an inventory of assessed vulnerabilities of the network 14." The Examiner interprets this to be a storage device storing event information.

Claim 31:

Paragraph [0012] teaches a firewall, IDS, and VAS system integrated into one system. The Examiner interprets this as three security engines communicating. Paragraph [0013] further states "the present invention integrates a network discovery functionality, an intrusion detector functionality and a firewalling functionality together such that a self-deploying and self-hardening security defense is provided for a network. Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations." This further teaches three integrated security engines.

Claim 32:

Paragraph [0012] teaches a firewall, IDS, and VAS system integrated into one system. The Examiner interprets this as three security engines communicating. Paragraph [0013] further states "the present invention integrates a network discovery functionality, an intrusion detector functionality and a firewalling functionality together such that a self-deploying and self-hardening security defense is provided for a network. Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations." This shows at least two different security services that are associated with at least two different types of security attacks.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 8-13, and 22-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Willebeek-Lemair** as applied to claims 14-17, 19-21, and 28-32 above, and further in view of **Chen (US 4, 970, 504)** hereinafter Chen.

Claims 1 and 2:

Willebeek-LeMair paragraph [0014] teaches an intrusion detector functionality that sends an alert when detecting potentially harmful traffic. This is sent to a firewall, which responds by blocking the entrance of the detected traffic. The Examiner interprets

the intrusion detector and firewall to be "security engines" of claim 1. This would then teach one security engine (intrusion detector) detecting an event (potentially harmful traffic), identifying a second security engine (firewall), and communicating the event to it.

Willebeek-LeMair does not teach but Chen teaches "the event corresponds to identifying a password that does not comply with a predetermined criteria" in Chen column 4 lines 11-31. The motivation to combine the two systems would be Chen column 4 lines 11-31 wherein the password being incorrect is an alarm condition in a security system and ways to determine the password being incorrect is when the "keyed-in password does not equal the currently stored password, including unequal number and inconsistent length".

Claim 3:

Willebeek-LeMair paragraph [0063] states that, "detection signatures 132 are supplied to the agent 126 either at the initiative of the network administrator 142, or in response to a request from the agent triggered by a threat detection by the network discovery functionality 112." Paragraph [0064] states that "before the detection signature 132 (more specifically, the machine code related thereto) is installed in the intrusion detection functionality 116 and/or firewalling functionality 118, the agent 126 may first query 134 the network discovery functionality." The Examiner interprets this as the communication of an event which is an action preformed by the agent in response to a security attack as in claim 3.

Willebeek-LeMair paragraph [0012] teaches a security engine as a vulnerability assessment scanner, which is equivalent to a vulnerability analysis application program.

Claim 4:

Willebeek-LeMair paragraph [0012] states "the present invention addresses the foregoing and other concerns with a single vendor solution that integrates the functionalities performed by a firewall, IDS, and VAS for network security into one system or appliance supported on a single platform." The abbreviations IDS and VAS are further explained in paragraph [0008] to mean intrusion detection system and vulnerability assessment scanner respectively. It would be obvious to a person skilled in the art at the time of invention that a "firewall, IDS, and VAS" could be implemented as application programs.

Claim 5:

Willebeek-LeMair does not teach but Chen teaches "the event corresponds to identifying a password that does not comply with a predetermined criteria" in Chen column 4 lines 11-31. The motivation to combine the two systems would be Chen column 4 lines 11-31 wherein the password being incorrect is an alarm condition in a security system and ways to determine the password being incorrect is when the "keyed-in password does not equal the currently stored password, including unequal number and inconsistent length".

Claim 8:

Willebeek-LeMair paragraph [0012] teaches a security engine as a vulnerability assessment scanner, which is equivalent to a vulnerability analysis application program.

Claim 9:

Willebeek-LeMair paragraph [0012] teaches a firewall, IDS, and VAS system integrated into one system. The Examiner interprets this as three security engines communicating. Paragraph [0013] further states "the present invention integrates a network discovery functionality, an intrusion detector functionality and a firewalling functionality together such that a self-deploying and self-hardening security defense is provided for a network. Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations." This further teaches three integrated security engines.

Claim 10:

Willebeek-LeMair paragraph [0064] teaches an agent that has received a detection signature scanning the network to determine if the detection signature is relevant to other parts of the network. The Examiner interprets the detection signature (defined in paragraph [0030] as "comprising, for example, security rules, policies and algorithms") to be equivalent to a "security policy" as in claim 10.

Claim 11:

Willebeek-LeMair paragraph [0063] states "the detection signatures 32 are supplied to the agent 126 either at the initiative of the network administrator 142, or in response to a request from the agent triggered by a threat detected by the network discovery functionality." The Examiner interprets this to be a request from one security engine for data and the communication of that data to it.

Claim 12:

Willebeek-LeMair paragraph [0075] teaches a "enterprise vulnerabilities databases that stores the enterprise specific data collected b y the network discovery functionality." It later states that the stored data may comprise "an inventory of assessed vulnerabilities of the network 14."

Claim 13:

Willebeek-LeMair paragraph [0012] teaches a "single vendor solution" integrating the security components. This could be interpreted by one of ordinary skill in the art at the time of invention to be a computer program.

Claim 22:

Willebeek-LeMair paragraph [0053] states, "the system 10 includes a security management agent 126 that functions to configure, tune and monitor the operation of the intrusion detector functionality 116 and the firewalling functionality 118." The Examiner interprets this to be equivalent to an event manager that receives and communicates alerts between two security engines.

Willebeek-LeMair does not teach but Chen teaches "the event corresponds to identifying a password that does not comply with a predetermined criteria" in Chen column 4 lines 11-31. The motivation to combine the two systems would be Chen column 4 lines 11-31 wherein the password being incorrect is an alarm condition in a security system and ways to determine the password being incorrect is when the "keyed-in password does not equal the currently stored password, including unequal number and inconsistent length".

Claim 23:

Willebeek-LeMair paragraph [0014] states "content that is potentially harmful to the network." The Examiner interprets this to be "a type of security attack" as in claim 23.

Claim 24:

Willebeek-LeMair paragraph [0063] states that, "detection signatures 132 are supplied to the agent 126 either at the initiative of the network administrator 142, or in response to a request from the agent triggered by a threat detection by the network discovery functionality 112." Paragraph [0064] states that "before the detection signature 132 (more specifically, the machine code related thereto) is installed in the intrusion detection functionality 116 and/or firewalling functionality 118, the agent 126 may first query 134 the network discovery functionality." The Examiner interprets this as the communication of an event which is an action preformed by the agent in response to a security attack as in claim 24.

Claim 25:

Willebeek-LeMair paragraph [0075] teaches that the network discovery functionality maintains a database that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information.

Claim 26:

Willebeek-LeMair paragraph [0012] teaches a firewall, IDS, and VAS system integrated into one system. The Examiner interprets this as three security engines

communicating. Paragraph [0013] further states "the present invention integrates a network discovery functionality, an intrusion detector functionality and a firewalling functionality together such that a self-deploying and self-hardening security defense is provided for a network. Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations." This further teaches three integrated security engines.

Claim 27:

Willebeek-LeMair paragraph [0075] teaches an "enterprise vulnerabilities databases that stores the enterprise specific data collected by the network discovery functionality." It later states that the stored data may comprise "an inventory of assessed vulnerabilities of the network 14." The Examiner interprets this to be a storage device storing event information. It is shown in Figure 2 that the database 140 is accessible to the security management agent 126.

Response to Arguments

Applicant's arguments, filed October 16, 2007, with respect to the rejection(s) of claim(s) 1-5, 8-17, and 19-32 have been fully considered and are persuasive. Therefore, the rejections based on commonly assigned prior art Cedar et al. (US 2003/0236994) has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Chen (US 4,970,504).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
1/24/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100